CLAIMS

What is claimed is:

1. A method comprising:

within a first device, generating data for permanent storage in a protected area of internal memory of the first device that prevents subsequent modification of the data; and

within the first device, producing a secret value being a combination of both (1) the data and (2) a short term value generated in response to a periodic event.

2. The method of claim 1 wherein prior to producing the secret value, the method further comprises:

performing the periodic event; and

generating the short term value

3. The method of claim 1, wherein the periodic event includes a power-up sequence by a platform employing the first device.

4. The method of claim 3, wherein prior to generating the data, the method further comprises:

transmitting a first command from a second device to the first device.

5. The method of claim 4, wherein prior to producing the secret value, the method further comprises:

transmitting the data to the second device.

6. The method of claim 5, wherein prior to producing the secret value, the method further comprises:

transmitting a second command from a second device to the first device; and

generating the short term value internally within the first device in response to the second command.

7. The method of claim 6, wherein prior to or concurrently with producing the secret value, the method further comprises:

transmitting the short term value to the second device.

8. The method of claim 1, wherein the combination is a result produced by successively performing a hash operation on both the data and the short term value.

9. A method comprising:

generating a long term value within a first device;

permanently storing the long term value within a protected area of an internal memory of the first device;

providing the long term value to a second device communicatively coupled to the first device;

generating a short term value within the first device, the short term value is modified after each periodic event;

providing the short term value to the second device;

generating a secret value within the first device, the secret value being a combination of both the long term value and the short term value; and

generating the secret value within the second device based on the long term value and the short term value.

10. The method of claim 9, wherein the periodic event includes a power-up sequence by a platform employing the first device.

11. The method of claim 9, wherein prior to generating the long term value, the method further comprises:

transmitting a first command from the second device to the first device.

12. The method of claim 9, wherein the long term value is generated in response to an initial power-up sequence when the first device is in communication with the second device.

13. The method of claim 12, wherein prior generating the short term value, the method further comprises:

transmitting a second command from the second device to the first device.

14. The method of claim 9, wherein the combination is a result produced by successively performing a hashing operation on both the data and the short term value.

15. A platform comprising:
a link;
an input/output control hub (ICH) coupled to the link; and
a trusted platform module (TPM) coupled to the link, the TPM including
a package,
an asymmetric key generation unit contained within the package, the asymmetric key generation unit to generate a long term value and a short term value, and
an internal memory contained within the package, the internal memory to permanently store the long term value and to temporarily store the short term value and a secret value being a combination of the long term value and the short term value.

16. The platform of claim 15, wherein the ICH including an internal memory.

17. The platform of 16, wherein the TPM transmits the long term value to the ICH over the link during manufacture of the platform and transmits the short term value to the ICH over the link in response to a power-up sequence by the platform.

18. The platform of claim 15, wherein the asymmetric key generation unit of the TPM includes a number generator.

19. The platform of claim 15, wherein the TPM further comprises a cryptographic engine performing a successive hashing operation on both the long term value and the short term value to produce the secret value.

20. A device comprising:
an internal memory; and
an asymmetric key generation unit to generate, in response to an initial event, a unique long term value for permanent storage in a protected area of the internal memory

and to generate, in response to a periodic event, a short term value for storage in the internal memory; and

a cryptographic engine to produce a secret value by combining both the long term value and the short term value.

21. The device of claim 20, wherein the periodic event includes a power-up sequence by a platform employing the device.

22. The device of claim 20, wherein the initial event includes an initial power-up sequence of the device when in communication with another device.

23. The device of claim 20, wherein the internal memory includes a non-volatile memory and a volatile memory.

24. The device of claim 20, wherein the cryptographic engine performs successive hashing operations on the long term value and the short term value when combining the long term value and the short term value.

25. A program loaded into platform readable memory for execution by a first device of a platform, the program comprising:

code to generate data for permanent storage in a protected area of internal memory of the first device in response to an initial event; and

code to produce a secret value being a combination of both the data and a short term value that is generated in response to a periodic event.

26. The program of claim 25 further comprising:

code to generate the short term value in response to a periodic event.

27. The program of claim 25, wherein the periodic event includes a power-up sequence by the platform.

28. The program of claim 25, wherein the initial event is a first power-up sequence after the first device is in communication with a second device of the platform for which the secret value is generated to create at least one secure communication channel between the first device and the second device.